

Appl. No. 09/360,575

Reply to Office Action of: May 17, 2005

REMARKS

Applicant wishes to thank the Examiner for reviewing the present application.

Claim Numbering

The originally filed claims included claims 1-8, none of which being numbered as claim 2. The claims added in the amendment filed February 3, 2004 were thus numbered 9-19, and claim 2 identified as "not presented". In the Office Action dated May 17, 2005, the Examiner refers to claims 8-18. Therefore, in the following remarks, Applicant will refer to claim 9 listed above as claim 8 consistent with the Examiner's numbering, and claim 10 as claim 9, etc.

Amendments to the Claims

Claim 8 (claim 9 listed above) is amended to incorporate the first and second messages recited in claims 12 and 13 (claims 13 and 14 listed above) and to indicate that the digital signature is obtained using the second message and that the payment is obtained using the digital signature. The steps are renumbered to include the new steps of sending the first and second messages. Accordingly, claims 12 and 13 are amended to delete the subject matter introducing the first and second messages, and to further define the information contained in these messages, namely to include credentials and details of the respective participants.

Claim 14 (claim 15 listed above) is amended to change its dependency to claim 9 (claim 8 is listed as claim 9 above), and to refer to step e) in view of the amendments to claim 8 (claim 9 listed above).

Claims 15 and 16 (claims 16 and 17 listed above) are amended inserting "said" before "payment" on the last line of each claim.

No new matter is believed to have been added by way of these amendments.

Claim Rejections – 35 U.S.C. §103

Claims 8-13, 17 and 18 have been rejected under 35 U.S.C. §103(a) as being unpatentable over US Patent No. 5,396,558 to Ishiguro et al. in view of US Patent No. 6,069,952 to Saito et al. Applicant respectfully traverses the rejections as follows.

Claim 8 (claim 9 listed above) is amended as described above, and in part requires the following step:

Appl. No. 09/360,575

Reply to Office Action of: May 17, 2005

e) upon verification of said information pertaining to said first participant, said second participant obtaining a digital signature for said first participant on said transaction using said second message, whereby said second participant may obtain said payment from a third participant using said digital signature.

Ishiguro teaches a method for performing a transaction with an IC card and a terminal. The method involves successive passes of card and terminal information wherein a digital signature is verified on each pass. Ishiguro does not teach obtaining a digital signature for the card to use for receiving a payment from a third participant (i.e. step e) above). The Examiner has indicated that Ishiguro does not teach such a step. However, the Examiner believes that Saito teaches the provision of a three participant transaction method having a third participant pay a second participant, and that Saito teaches the provision of a digital signature being attached to any of the communications.

Saito teaches a transaction system and method, involving a bank, customer, and retail shop as shown in Figure 8 and described in columns 39-42. Essentially, the customer uses a terminal to request an amount of digital cash from the bank and sends a customer ID number. The bank receives the request and encrypts the cash with a first key. The customer receives the encrypted amount and confirms the content using the first key. The customer generates a second key and encrypts the cash with the same. The customer may then decrypt the cash using the second key when a purchase is conducted. The retail shop receives the encrypted cash from the customer and obtains the second key through its bank and the customer's bank. The retail shop obtains the second key and decrypts the cash to confirm the amount. Once confirmed, an article of desire is transferred to the customer.

Saito indicates in column 42, lines 55-58 that digital signatures are beneficial during any of the above communications. The Examiner believes that it is possible to find each of the claimed steps by selectively combining Saito and Ishiguro, so that the steps of having each participant verify each other and the second participant obtaining a digital signature for effecting payment, can be found. Applicant respectfully disagrees.

Applicant believes that if one were to combine Saito with Ishiguro, at best, the method taught by Ishiguro could be modified to include the additional step of receiving a payment by obtaining a decryption key from a third entity. However, Ishiguro does not suggest how his

Appl. No. 09/360,575

Reply to Office Action of: May 17, 2005

system could be implemented using a third entity, let alone incorporating the exchange of a decryption key and decrypting electronic cash. Therefore, step e) is not taught by the combination of Ishiguro and Saito, and there is no motivation to make such a combination.

Amended claim 8 (claim 9 listed above) includes a verification of each participant involving the exchange of respective messages. The messages are used to verify the other participant's identity to ensure the service will be performed. Once the verification steps have been completed, the second participant obtains a digital signature for the first participant on the transaction using the message sent by the first participant. Using this digital signature, the second participant may obtain payment from a third participant, e.g., a bank.

Neither Ishiguro nor Saito teach a step of obtaining a digital signature on a message sent from the first participant to the second participant, wherein the digital signature is used to obtain payment from a third participant. Only Saito includes a third participant (e.g. the bank) that provides a decryption key to the second participant for decrypting the cash. Moreover, Saito only mentions that using a digital signature on an exchange of information provides increased security, not how the signature is obtained or used.

Therefore, Applicant respectfully submits that claim 8 (claim 9 listed above) clearly distinguishes over the combination of Ishiguro and Saito. Claims 9-18 (claims 10-19 listed above) in their dependencies on claim 8 are also believed to distinguish over the prior art cited by the Examiner.

Claims 14-16 (claims 15-17 listed above) have been rejected under 35 U.S.C. §103(a) as being unpatentable over US Ishiguro view of Saito, in further view of US Patent No. 5,276,736 to Chaum. Applicant respectfully traverses the rejections as follows.

Claims 14-16 are ultimately dependent on claim 8. Applicant has shown above that neither Ishiguro nor Saito teach step e) of amended claim 8. Therefore, Chaum must at least teach what is missing from Ishiguro and Saito.

Chaum teaches the provision of a "challenge" wherein a digital signature is obtained based on the messages exchanged during the challenge. However, Chaum does not teach a step of obtaining a digital signature on a message sent from the first participant to the second participant, wherein the digital signature is used to obtain payment from a third participant. Therefore, for at least that reason, claims 14-16 are believed to clearly and patentably distinguish over the prior art cited by the Examiner.

Appl. No. 09/360,575

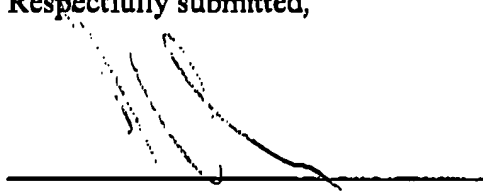
Reply to Office Action of: May 17, 2005

Summary

In view of the foregoing, Applicant respectfully submits that claim 8-18 (claims 9-19 listed above) clearly and patentably distinguish over the prior art cited by the Examiner, and as such are in condition for allowance.

Applicant requests early reconsideration and allowance of the present application.

Respectfully submitted,



John R.S. Orange
Agent for Applicant
Registration No. 29,725

Date: Nov. 17, 2005

BLAKE, CASSELS & GRAYDON LLP
Suite 2800, P.O. Box 25
199 Bay Street, Commerce Court West
Toronto, Ontario M5L 1A9
CANADA

Tel: 416.863.3164
JRO/BSL